This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-123. (Canceled)

124. (Currently Amended) The ~~medium~~ method of claim ~~121~~ 136 wherein the license provider location is an Internet address.

125. (Canceled)

126. (Currently Amended) The ~~medium~~ method of claim ~~121~~ 136 wherein the content provider public key is encrypted according to the decryption key (KD).

127. (Currently Amended) The ~~medium~~ method of claim 126 wherein the encrypted content provider public key is signed by the content provider private key, and wherein alteration of the encrypted content provider public key prevents validation of the digital content package.

128. (Currently Amended) The ~~medium~~ method of claim ~~121~~ 136 wherein the content provider public key is signed by the content provider private key, wherein alteration of the content provider public key prevents validation of the digital content package.

129. (Currently Amended) The ~~medium~~ method of claim ~~121~~ 136 further comprising a fifth data field containing a key ID identifying the decryption key (KD).

130. (Currently Amended) The ~~medium~~ method of claim ~~121~~ 136 wherein the digital content package is provided by a content provider authorized by a root source to provide the digital content package, the digital content package further comprising a fifth data field containing a certificate from the root source indicating that the content provider has authority from the root source to provide the digital content package.

131. (Currently Amended) The ~~medium~~ method of claim 130 wherein the content provider has a public key and a private key, and wherein the certificate includes the public key of the content provider.

132. (Currently Amended) The ~~medium~~ method of claim 131 wherein the root source has a public key and a private key, wherein the certificate is signed with the private key of the root source, and wherein the public key of the root source must be obtained to decrypt the encrypted signature.

133. (Currently Amended) The ~~medium~~ method of claim ~~121~~ 136 wherein the digital content package is provided by a content provider authorized by an intermediary source to provide the digital content package, the intermediary source in turn being authorized by a root source to authorize the content provider, the digital content package further comprising a fifth data field containing a first certificate from the root source indicating that the intermediary source has authority from the root source to authorize the content provider, and a sixth data field containing a second certificate from the intermediary source indicating that

the content provider has authority from the intermediary source to provide the digital content package.

134. (Currently Amended) The ~~medium~~ method of claim 133 wherein the content provider has a public key and a private key, wherein the intermediary source has a public key and a private key, wherein the first certificate includes the public key of the intermediary source, and wherein the second certificate includes the public key of the content provider.

135. (Currently Amended) The ~~medium~~ method of claim 134 wherein the root source has a public key and a private key, wherein the first certificate is signed with the private key of the root source, wherein the second certificate is signed with the private key of the intermediary source, wherein the public key of the root source must be obtained to decrypt the encrypted signature of the first certificate, and wherein the public key of the intermediary source is obtained from the first certificate to decrypt the encrypted signature of the second certificate.

136. (New) A method for using digital rights management to enforce rights in digital content, the digital content located in a digital content package, the method comprising:

distributing the digital content package from a content server to a computing device of a user, wherein the digital content package is provided to the content server by a content provider having a public key and a private key, wherein the digital content package comprises:

a first data field containing the digital content to be rendered in accordance with a corresponding digital license, the digital content being encrypted, the digital content being decrypt-able according to a decryption key (KD) obtained from the corresponding digital license;

a second data field containing a content ID or a package ID identifying one of the digital content and the digital content package respectively, the corresponding digital license also having the content ID or the digital content package ID such that the content ID or the digital content package ID from the digital content package is employed to locate the corresponding digital license;

a third data field containing license acquisition information including a location of a license provider for providing the license after identifying the digital content ID or the digital content package ID to the license provider, wherein the license acquisition information is in an unencrypted form; and

a fourth data field containing the content provider public key, wherein the corresponding license including a content provider digital certificate issued and signed by the content provider private key to show permission from the content provider to the license provider to provide the corresponding digital license, such that the content provider public key from the digital content package is employed to validate the content provider digital certificate of the corresponding digital license;

receiving the distributed digital content package at the computing device;

attempting to render the digital content by way of a rendering application;

invoking, by the rendering application, a Digital Rights Management (DRM) system upon the rendering application attempting to render the digital content, the DRM system employing a trusted black box to perform decryption and encryption functions;

determining, by the DRM system, whether a right to render the digital content in the manner sought exists based on any digital license stored in the computing device and corresponding to the digital content; and

if the right does not exist:

requesting from a license server a particular digital license that corresponds to and is separate from the digital content;

issuing, by the license server, the particular digital license to the DRM system only if the license server trusts the DRM system to abide by the particular digital license;

receiving, by the computing device and from the license server, the issued particular digital license corresponding to the digital content;

storing the received particular digital license on the computing device; and

rendering the digital content using the rendering application and the stored particular digital license.